REMARKS

Claims 1-22 and 35 remain in the application. Claims 1, 3, 6-7, 10 and 18-20 were amended for clarity. No new matter has been added.

Alleged New Matter

The Office action alleged that the amendment of 03 October 2005 introduced new matter into the disclosure because "Applicant has not shown support in the specification for the added material in the amendment." However, the amendment of 03 October 2005 clearly has support in the specification as originally-filed since claims are part of the specification and, as previously submitted, the amendment was "to add a summary of the canceled claims" to the specification. As such, the Office action requirement for Applicants to cancel the alleged new matter is erroneous, and Applicants request reconsideration and withdrawal of the objection.

Claim Rejections - 35 USC 102

Claims 1-15, 19, 20 and 22 were rejected as allegedly being anticipated by He. However, to anticipate a claim, the reference must teach every element of the claim:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

In the present case, numerous claim elements are not found in He.

Independent claim 1 requires "providing an intelligent network interface *between* a network and *each node* on the network," yet no such intelligent network interfaces are disclosed in He between user nodes **14** and network **10**. The Office action states that "[e]ach network element has an interface to the network through its own terminal server..." However, Applicants note that the network elements in He are switches,

mainframes, databases, etc. and clearly do not include the user nodes or user devices ("user nodes 14" in He). As such, each node in He does *not* have a terminal server between it and the network and therefore He cannot anticipate the claim.

Independent claim 1 further requires "encrypting and decrypting critical data transmissions over the network using said intelligent network interfaces." However, since He does not have intelligent network interfaces (as discussed above), it cannot perform this step. Instead, He relies upon a central Security Server **15** for this function (see data encryption module **54** in **figure 2**). Independent claim 1 also requires "centrally managing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network with a central management console." Again, since He does not disclose intelligent network interfaces or encryption by said interfaces, this element is not found in He. In view of He's failure to disclose numerous claim elements, Applicants submit that He cannot anticipate claim 1 or any of the claims dependent thereon and requests reconsideration and withdrawal of the rejection.

Claim 10 requires "providing an intelligent network interface between a network and each device on the network" where each device on the network includes "user's host device." As with claim 1, He cannot disclose "an intelligent network interface between a network and each device on the network" since no such interfaces are provided to user nodes 14. Because of this, He also lacks any disclosure of "a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device." In view of He's failure to disclose numerous claim elements, Applicants submit that He cannot anticipate claim 10 and requests reconsideration and withdrawal of the rejection.

Similarly, independent 11 requires "an intelligent network interface between each host device and said network," yet no such intelligent network interfaces are disclosed in He between user nodes **14** and network **10**. Independent claim 11 further requires "means on each intelligent network interface for encrypting and decrypting critical data transmissions over the network." However, since He does not have intelligent network interfaces (as discussed above), it cannot perform this step. Instead, He relies upon a central Security Server **15** for this function (see data encryption module **54** in **figure 2**).

Independent claim 11 also requires "at least one central management console for providing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network." Again, since He does not disclose intelligent network interfaces or encryption by said interfaces, this element is not found in He. In view of He's failure to disclose numerous claim elements, Applicants submit that He cannot anticipate claim 11 or any of the claims dependent thereon and requests reconsideration and withdrawal of the rejection.

Indeed, Applicants respectfully submit that the present invention uses a different security model than He. Whereas the presently-claimed invention uses intelligent network interfaces to perform authentication, encryption and other security functions, He uses a central security server to perform these functions. While He does use terminal security servers to work with the central security server, any user login or session initiation is done by having the user login to the central security server. In the presently-claimed invention, a central management console is used to push policy information to the individual secure intelligent network interfaces. However, the intelligent network interfaces are then able to perform functions such as user login, access control, and encryption directly with other intelligent network interfaces. The implications of the differences of these two models is significant. In the present invention, intelligent network interfaces can enforce login and communication policies with each other even when the CMC is not available as long as the CMC has previously loaded the necessary policy information or servlets to the intelligent network interfaces. If the Security Server in He is unavailable, the system no longer works.

With respect to claim 1, the Office action points out that in He, "the security server performs all network security functions for the network including ..." In contrast, the security services of claim 1 of the present invention are not performed by a central server. Rather, such functions are performed by the intelligent network interfaces.

With respect to claims 2, 4, and 5, Applicants note various deficiencies in He. First, each user node 14 does not have its own terminal server. Indeed, all users in He must login to the central security server before the subservient terminal servers can perform their services. In contrast, the present invention works between intelligent network interfaces (i.e., on a peer to peer basis) so it can provide protocol translation,

proxy services, etc. without intervention from the CMC. Indeed, the CMC dynamically distributes servlets, which is nowhere taught or suggested by He. While elements of He may act as gateways or bridges (i.e., the terminal servers 24), no code is distributed from a CMC. In He, the Security Server 15 provides authorization, user privilege control, user access auditing, data integrity, etc., so it has no need to distribute code to perform such services as protocol translation, proxies, firewalls, auditing, policy enforcement, and web filtering.

With respect to claim 3, mere disclosure of an IP network does not disclose protocol translation within a layer or the distribution of servlets to provide the translation, both of which are absent from He.

With respect to claim 6, the examiner explicitly points out that in He "the security server performs all network security functions for the network..." This is the opposite of the claimed method, where the security functions are performed by the decentralized intelligent network interfaces.

With respect to claims 7, Applicants submit that He's disclosure of KERBEROS does not anticipate the claimed use of an IPSec Security Parameters Index.

With respect to claims 8, the presently-claimed method is distinguished from the He method in that the authentication is handled by the decentralized intelligent network interface, not the central security server as in He.

With respect to claim 9, the fact that a single Security Server of He contains a plurality of security mechanisms has nothing to do with providing a plurality of CMCs in a hierarchical configuration. If anything, it teaches against the presently-claimed invention, i.e., that a single device can provide multiple functions, which teaches away from a hierarchical set of CMCs. The significance of using a hierarchy of CMCs is that it allows organizations to provide hierarchical control over policy creation and dissemination that reflects the hierarchy of responsibility in their organization.

With respect to claim 10, Applicants note that the presently-claimed single sign-on authentication and security policy enforcement are done at the intelligent network interfaces attached to network nodes. In He these functions are done by a central security server. While He does use a terminal server to connect network elements to the network and send information to the central server, these interfaces cannot perform policy

enforcement independently of the central server. In the present invention, the CMC does not do policy enforcement, encryption, or management of session keys. It is used for the creation and dissemination of the policy to be enforced by the intelligent network interfaces.

With respect to claim 11, the examiner states that "the security server performs all network security functions for the network including data encryption for authentication information and regular traffic." While this is the case with He, the presently-claimed invention is distinctly different since these functions are performed by the individual intelligent network interfaces based on policy information dynamically distributed (pushed) from the CMC. The CMC plays no role in performing these functions after the policy has been pushed to the intelligent network interfaces. In fact, these devices will continue to function and enforce the policy even if the CMC is removed from the network.

With respect to claims 12 and 19, Applicants note that the CPU, memory and interfaces as claimed are part of the intelligent network interfaces, not the user computer. It is this separation that allows the intelligent network interfaces to operate transparently and in isolation from standard user applications. The CPU and memory are used in intelligent network interfaces because it is the primary enforcement point for network security policies. He does not disclose this separation.

With respect to claims 13,14, and 20, Applicants note that, while the terminal server of He and intelligent network interfaces can both be standalone devices, they play different roles in enforcing network security policies. The He terminal server, as the name suggests, is simply an interface to support communication with a central security server and perform some limited part of security functions based on security server direction about a specific session. On the other hand, present invention envisions an intelligent interface that is capable of enforcing policy on a peer to peer basis independent of a central security server other than receiving policy requirements.

With respect to claim 15, Applicants again note that each user node or device of He does not have its own terminal server and just because the terminal server of He has a serial interface does not mean it has a "serial line *authentication* port" as required by the

claim. Indeed, authentication in He is performed at security server 15 such that there is no need for one at terminal server 24.

And with respect to claim 22, Applicants submit that He lacks any disclosure of dynamically distributed code fragments. In He, the user logs into the central server which can then distribute data for security (not code fragments). In the present invention, the CMC can download policy and code fragments but the individual intelligent network interfaces then perform security functions and policy enforcement on a peer to peer basis.

In view of the above arguments, Applicant respectfully submits that claims 1-15, 19, 20, and 22 are novel and non-obvious over the cited prior art.

Claim Rejections - 35 USC 103

Claim 16 was rejected as being obvious over He in view of Liu. However, implicit in this rejection is the assumption that He discloses everything except a USB serial port. As discussed above with respect to anticipation, He fails to disclose numerous claim limitations. In order to establish a prima facie case of obviousness, the prior must teach or suggest **all** the claim limitations (see M.P.E.P. Section 2143), yet the combination of He and Liu fails to teach or suggest all of the missing limitations discussed above with respect to the anticipation rejections.

Claim 17 was rejected as being obvious over He. However, implicit in this rejection is the assumption that He discloses everything except a parallel port. The claim actually requires a parallel port *authentication port on the intelligent network interface.* He discloses authorization on security server 15 and an ordinary serial port on terminal server 24, neither of which are an "intelligent network interface" as presently claimed.

Further, as discussed above with respect to anticipation, He fails to disclose numerous claim limitations. In order to establish a prima facie case of obviousness, the prior must teach or suggest **all** the claim limitations (see M.P.E.P. Section 2143), yet He fails to teach or suggest all of the missing limitations discussed above with respect to the anticipation rejections.

Claim 18 was rejected as being obvious over He in view of Kitazaki. As before, implicit in this rejection is the assumption that He discloses everything except storing an OS on flash memory. In fact, the claim does not merely require storing an OS on flash memory, but rather requires that the memory in an intelligent network interface that is attached to every host device on a network use flash memory for storing an OS and dynamic memory for applications. Kitazaki discloses that OS and applications use the same flash memory (see 14b of Fig. 1) and thus, even if properly combinable, does not disclose the claim limitation.

Additionally, as discussed above with respect to anticipation, He fails to disclose numerous claim limitations. In order to establish a prima facie case of obviousness, the prior must teach or suggest **all** the claim limitations (see M.P.E.P. Section 2143), yet the combination of He and Kitazaki fails to teach or suggest all of the missing limitations discussed above with respect to the anticipation rejections.

Claim 21 was rejected as being obvious over He in view of Walter. However, implicit in this rejection is the assumption that He discloses everything except an encryptor on an FPGA. As discussed above with respect to anticipation, He fails to disclose numerous claim limitations. In order to establish a prima facie case of obviousness, the prior must teach or suggest **all** the claim limitations (see M.P.E.P. Section 2143), yet the combination of He and Walter fails to teach or suggest all of the missing limitations discussed above with respect to the anticipation rejections.

In view of the above arguments, Applicant respectfully submits that claims 16, 17, 18, and 21 are novel and non-obvious over the cited prior art.

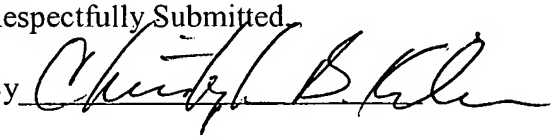
Allowable Claims

While the Office action failed to include any reasoning with respect to a rejection of claim 35 it is anticipated that the Examiner would have applied the references cited in the other rejected claims. In the absence of a basis for a rejection, Applicants respectfully assert the above reasoning similarly applies to the elements of claim 35 as previously presented. For the reasons noted above, Applicants respectfully request allowance of claim 35.

Conclusion

For the reasons cited above, Applicants submit that claims 1-22 and 35 are in condition for allowance and requests reconsideration of the application. If there remain any issues that may be disposed of via a telephonic interview, the Examiner is kindly invited to contact the undersigned at the local exchange given below.

Respectfully Submitted,

By 

Jon L. Roberts, Esq.
Registration No. 31,293
Christopher B. Kilner, Esq.
Registration No. 45,381
Roberts Mardula & Wertheim, LLC
11800 Sunrise Valley Drive, Suite 1000
Reston, VA 20191
703-391-2900